Random Number Flow and Its Uses in Confidentiality and Encryption of Electronic Messages

Kanashvili, Mariam

Meskhi, Giorgi

Keeping information safe has been neither as vital nor urgent as it is now. Because of the worldwide problem of technological confidentiality, we were concerned and motivated to investigate an easily, usable and, cheap method of defending electric messages. Our proposed method is to encrypt a message using a random numbers flow algorithm in a new and original way, comparable to, though independent of, the one-time pad (OTP) technique. The unique specifications of the machine sending the message is used as the source of random number flow, rather than having the algorithm generate the numbers itself. The encryption process uses text tabulation as a classical movable and/or unchanging cipher. Our proposed method is structured based on the of an algorithm that can be easily implemented on a wide variety of devices; even in the case of multiple/differing phone providers and phone capabilities, it can still provide users with practical and efficient confidentiality during private conversations. The method is simple and inexpensive, without any need of extensive technical equipment. At the same time, breaking the encryption requires a great expenditure of both time and monetary resources; and, even when broken, the algorithm uses a disposable, one-use encryption code and cannot be reused to crash another message in the same way.

Awards Won: